Final Report: NCC 2-398

Matt Bishop

Introduction

The task *Improving Computer Security* consisted of three parts: a file monitoring subsystem for the computers on the NAS network, a more stringent program for granting superuser privileges on those machines, and a password analyzing program. The results and status of each are summarized below.

File Monitoring Subsystem

The subsystem is described in the attached report "Adding an Auditing Subsystem: A Retrospective." The subsystem has been in use for roughly two years and has been enhanced to perform remote audits as well as provide a convenient and comfortable user interface.

Paper: "Auditing Files on a Network of UNIX Machines," *Proceedings of the UNIX Security Workshop*, Portland, OR (August 29-30, 1988) pp. 51-52

Controlling Access to the Superuser

The program developed now allows access to the superuser to be conditioned not merely on knowledge of the superuser password, but also on the basis of the account from which the enabling of privileges is attempted, the time of day, and the terminal involved. A related program allows access to group accounts based on the user's knowledge of his or her own password and on the other constraints given above; with accounts other than *root*, this solves the problem of password distribution. (The mechanism is not secure enough to use fot *root*.)

Paper: "Sharing Accounts," *Proceedings of the Large Installation System Administrtors Workshop*, Philadelphia, PA (April 9-10, 1988) pp. 36

Technical Report: "A Mechanism for Sharing Accounts," RIACS TR 87.10 (March 1987)

Password Analysis and Checking

A set of library routines to implement the UNIX password encryption algorithm efficiently were written, as well as software to allow the password files to be checked. Software to force the user to select a "good" password, "good" being determined by the site administration, were also developed, as was a file encryption program based on the Data Encryption Standard.

Paper: "An Application of a Fast Data Encryption Standard Implementation," *Computing Systems* 1(3) (Summer 1988) pp. 221-254

Technical Report: "A Fast Version of the DES and a Password Encryption Algorithm" RIACS TR 87.18 (July 1987, revised August 1988)

RIACS
Research Institute for Advanced Computer Science

Mail Stop 230-5
NASA Ames Research Center
Moffett Field, CA 94035
(415) 694-6363

January 17, 1989

NASA Scientific and Technical Information Facility
PO Box 8757
Baltimore/Washington International Airport
Maryland 21240

Dear Sirs:

Enclosed please find 2 copies of the Final Report for NASA Cooperative Agreement, Grant # NCC2-398.

No inventions resulted from research performed during this grant.

Sincerely,

Barbara Curlette

Barbara Curlette
Resource Analyst

Enclosures

cc: William Kramer, Grant Technical Monitor
B. Hastings, University Affairs Office
Jack Nielsen, RIACS Technical Monitor
M. Smith, RIACS Technical Monitor